



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

09/913,452

12/05/2001

Graeme John Proudler

B-4277PCT

9816

7590

11/02/2004

Richard P Berg  
Hewlett Packard Company  
IP Administration Mail Stop 35  
3404 East Harmony Road  
Ft Collins, CO 80528-9599

EXAMINER

DO, THUAN V

ART UNIT

PAPER NUMBER

2825

DATE MAILED: 11/02/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

## Office Action Summary

Application No.

09/913,452

Applicant(s)

PROUDLER ET AL.

Examiner

Thuan Do

Art Unit

2825

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

### Status

- 1) ☒ Responsive to communication(s) filed on 24 August 2004.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

### Disposition of Claims

- 4) ☒ Claim(s) 1-10, 12-17 and 22-54 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-10, 12-17, 22-54 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

### Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
  - ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

### Attachment(s)

- |  |   |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892)   | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)                                   | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152)             |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)<br>Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____  |

### **DETAILED ACTION**

1. This is final action responsive to amendment entered on 08/24/2004. Claims 1-10,12-17,22-54 are pending in this office action. Claims 11, 18-21 have been canceled.

#### ***Claim objections***

Claim 54, the term "private key" is unclear to what it means within specification. Clarification or correction is required.

#### ***Claim Rejections - 35 USC § 102***

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –  
(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

2. Claims 1-10,12-17,22-54 are rejected under 35 U.S.C. 102(b) as being unpatentable over Ginter et al., Pat. No. 5892900.

**Regarding claim 1:** Ginter teaches an apparatus comprising, mounted on an assembly, main processing means, main memory means and a trusted device, each being connected for communication with one or more other components on the assembly, the trusted device being arranged to acquire a true value of an integrity metric of the computing apparatus (col. 68, lines 29-42 ).

**Regarding claims 2-10,44-49:** These claims teach a similar apparatus of claim 1 and rejected in columns 68,76,78 and/or 79 as detailed in argument section.

**Regarding claim 12:** Ginter teaches a method comprising:  
the trusted device acquiring the true value of the integrity metric of the trusted computing apparatus (Figure 9 at least box 524) ;

Art Unit: 2825

the user generating a challenge for the trusted computing apparatus to prove its integrity and submitting the challenge to the trusted computing apparatus (col. 68, lines 29-42) ;

the trusted computing apparatus receiving the challenge, and the trusted device generating a response including the integrity metric and returning the response to the user apparatus (col. 19, lines 29-58 using evaluation process ) ; and

the user receiving the response, extracting the integrity metric from the response and comparing the integrity metric with an authenticated metric for the trusted computing apparatus that had been generated by a trusted party (col. 9, lines 19-30 using VDE extraction ).

**Regarding claim 13:** Ginter teaches a method with security algorithm (col. 45, lines 49-62).

**Regarding claims 14-17,50:** These claims teach a similar method of claim 12 and rejected in columns 68,76,78 and/or 79 as detailed in argument section.

**Regarding claim 22:** Ginter teaches computing apparatus comprising an assembly; a main processor, a main memory and a trusted device, each being mounted on the assembly and connected for communication with other components mounted on the assembly, wherein the trusted device is adapted to acquire a value of an integrity metric (figure 9 and col. 68, lines 29-42 ) that measures that the computing apparatus is operating as intended and determining the correctness of the acquired value of the integrity metric (col. 64, lines 1-15 for correctness determination ) .

**Regarding claims 23-43,51,52:** These claims teach a similar apparatus of claim 22 and rejected in columns 68,76,78 and/or 79 as detailed in argument section.

**Regarding claims 53 and 54:** Ginter teaches the functions and activities of smart cards at least in col. 8, lines 1-7 and col. 100, lines 35-45.

### ***Response to Arguments***

3. Applicant's arguments have been considered but are not persuasive for the following reasons:

Applicant said that Ginter does not teach the trusted device being arranged to acquire a true value of an integrity metric of the computing apparatus.

Ginter teaches computing devices (apparatus) for trusted security application arranged with processor, memory, assembly connections in figure 9 where the box 524 performs (acquire) pattern matching by comparing data for integrity metric data in col. 68, lines 28-42. This meets the claim limitation.

Applicant said that Ginter does not teach arranged to transfer the instructions of the program code to the main processing means.

Ginter teaches the instruction code is executed and transferred by SPU processor in col. 78, lines 56-67 that meets this claim limitation.

Applicant said that Ginter does not teach the first instructions executed after release from reset.

Ginter teaches the reset in col. 79, lines 35-40.

Applicant said that Ginter does not teach arranged to monitor a data bus means by which components mounted on the assembly are adapted to communicate and store in the device memory means a flag in the event the first memory read signals generated by the main processing means after the computing apparatus is released from reset are addressed to the trusted device.

Ginter teaches this feature in col. 76, lines 65-67.

Applicant said that Ginter does not teach generating a challenge for the trusted computer apparatus to prove its integrity" or "submitting the challenge to the trusted computing apparatus.

Ginter teaches this feature by computing devices (apparatus) for trusted security application arranged with processor, memory, assembly connections in figure 9 where the box 524 performs (acquire) pattern matching by comparing data in order to get the validation output for the concerned integrity metric data of a trusted computing apparatus in col. 68, lines 28-42.

Applicant said that Ginter does not teach returning the response to the user.

Ginter teaches this feature by control information of application events by user in col. 80, lines 55-60.

Applicant said that Ginter does not teach the integrity metric and the nonce, both digitally signed by the trusted device using a information security algorithm, and the user verifies the integrity metric and the nonce using a respective information security algorithm or determining the correctness of the acquired value of the integrity metric.

Within the above statement, Ginter teaches computing devices (apparatus) for trusted security application arranged with processor, memory, assembly connections in figure 9 where the box 524 performs (acquire) pattern matching by comparing (digitally and nonce for security algorithm functions) data in order to get the validation (correctness ) output for the concerned integrity metric data of a trusted computing apparatus in col. 68, lines 28-42. The column 45, lines 49-62 contains a SPU for security processing within system 500 of figure 9 apparatus.

This argument supports the claimed similarity of the above rejection and therefore the final rejection is written.

**THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than **SIX MONTHS** from the mailing date of this final action.

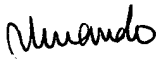
Art Unit: 2825

### **CONTACT INFORMATION**

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thuan Do whose telephone number is 571-272-1891. The examiner can normally be reached on Monday-Friday 8:30-4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Matthew S. Smith can be reached on 571-272-1907. The fax phone numbers for the organization where this application or proceeding is assigned are 703 305-3431 for regular communications and 703-305-3431 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-308-0596.



Thuan Do  
Primary examiner  
10/29/04